REMARKS

The Examiner has rejected Claims 1-2, 5-6, 8-12, 14-15, 17-19, 21-22, 24 and 26-31 under 35 U.S.C. 102(b) as being anticipated by Hitachi, Ltd. (EP 0893 769 A1). The Examiner has also rejected Claims 3, 4, 13, 20 and 23 under 35 U.S.C. 103(a) as being unpatentable over Hitachi in view of Arnold et al. (U.S. Patent No. 5,440,723). Applicant respectfully disagrees with such rejections.

With respect to independent Claims 1, 9-11, 17 and 23, the Examiner has relied on Col. 5, lines 21-39; Col., 8, lines 48-57 and steps 801-823 in Figure 8 of Hitachi to make a prior art showing of applicant's claimed technique "wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content."

In the latest action, the Examiner further argues that Hitachi discloses "scanning with a malicious code detection file received after the potentially malicious content." Specifically, the Examiner cites the excerpts below, along with items 613 and 652 from Fig. 6:

> "Referring to Fig. 8, description will be given of an operation in which the file 613 suspected for the infection of a virus is provisionally isolated by the file server 621 to prevent the infection with the computer virus of a new type through cooperation of the programs 651, 650, and 653 related to security.
>
> Next, description will be given of each step.
>
> (1) Pre-processing
>
> In step 801, the security agent 651 arrives at the computer 611 and then starts a search. In step 802, in accordance with a list 652 generated as a result of the previous circulation, the security agent 651 makes a search for a file 613 suspected for infection with a computer virus of a new type. As criteria for the suspected files, there may be used, for example, a new file generated after the previous circulation or a file updated also thereafter." (see col. 13, lines 25-43)

After carefully reviewing the above excerpt, however, it appears that the Examiner has still failed to take into consideration the full weight of applicant's claims.

Specifically, in Hitachi, the step 801 related to the search for a suspect file occurs prior to quarantine (see operation 804). To this end, it is impossible for such excerpt from Hitachi to meet applicant's claimed technique "wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content," (emphasis added), as claimed where the quarantine continues until the condition noted above.

In fact, the only action after the quarantine (and before the release of the quarantine in steps 812 et al.) is that of step 811. However, as noted from the description of such step 811, there is absolutely no quarantine "until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content" (emphasis added). Only applicant teaches and claims receiving a malicious code detection file after the potentially malicious content is received, such that the quarantine lasts until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content, as claimed.

With respect to the 102 rejection, the Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim. This criterion has simply not been met by the Hitachi reference, as noted above.

With respect to the 103 rejection, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991). Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest <u>all</u> of the claim limitations, as noted above.

Thus, a notice of allowance or a specific prior art showing of each of the foregoing claimed features, in combination with the remaining claimed features, is respectfully requested.

The Examiner continues by arguing with respect to Claim 4, that "Arnold discloses the use of estimated false positives see Col 9 Ln 61-68 and collecting of statistics regarding communications see Col 9 Ln 49-57. Arnold is suggestive of false positive of predetermined amount to be used to indicate when a incorrect assessment is made and thus limit release the amount of communications received."

In response, it appears that the Examiner has not taken into consideration the full weight of applicant's claims. Specifically, applicant respectfully asserts that the "predetermined threshold" from Arnold refers to "false-positives" associated with <u>signatures</u> and are used <u>to identify appropriate signatures</u>. In sharp contrast, applicant teaches and claims namely a technique "wherein <u>content is identified as potentially malicious</u> when a <u>number of instances of the content</u> in the network communications is greater than a predetermined value" (emphasis added). In other words, the predetermined value of the present claims are associated with <u>content in network communications</u> (not signatures, as in Arnold) and are used <u>to identify malicious communications</u> (not false-positives, as in Arnold).

In addition, with respect to Claim 6, the Examiner argues that 'Hitachi discloses the message being having a subject of "acceleration" or "suppression" to be used to determine whether malicious content has been sent see Fig. 1 item 120, 125 & Col 7 Ln

9-17 & Col 9 Ln 18-30.' However, after carefully reviewing such excerpts, it is noted that Hitachi does not even mention a subject line of a message, let alone "an electronic mail message [that] is identified as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value," as specifically claimed by applicant (emphasis added).

With respect to Claim 27, the Examiner now argues that "Hitachi discloses a messages to be placed on a list and further executing and forwarding of messages see Col 9 Ln 58- Col 10 Ln 37." Whether or not Hitachi discloses such, applicant's claim limitations would nevertheless not be met, since applicant's claim language specifically requires that each of the recipients (not mere messages) is placed in a list such that after the potentially malicious content is determined to be clean based on the testing, the single copy is forwarded to each of the recipients, as claimed.

Still yet, applicant disagrees with the Examiner's rejection of new Claims 29-31 below, as it appears that the Examiner has not taken the following emphasized limitations into full consideration.

> "wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with the malicious code detection file received after the potentially malicious content **and** after the potentially malicious content is quarantined" (see Claim 29);
>
> "wherein the malicious code detection file is created after the potentially malicious content is identified such that a latest malicious code detection file is utilized in the scanning of the potentially malicious content" (see Claim 30); and
>
> "wherein the malicious code detection file is created after the potentially malicious content is received such that a latest malicious code detection file is utilized in the scanning of the potentially malicious content" (see Claim 31).

As noted above (with respect to the arguments related to the independent claims), the potentially malicious content is not quarantined in Hitachi until the potentially malicious content has been scanned with the malicious code detection file received after the potentially malicious content, and thus is certainly not quarantined until the potentially malicious content has been scanned with the malicious code detection file received after the potentially malicious content is quarantined (emphasis added - note Claim 29).

For similar reasons, the aforementioned emphasized functionality of Claims 30-31 is simply not existent in the prior art as claimed, as they relate to advantages associated with the novel features of Claims 1 and 29 et al.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P040/01.254.01).

Respectfully submitted,
Zilka-Kotab, PC

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100